

UNITED STATES DISTRICT  
SOUTHERN DISTRICT OF NEW YORK

HERBALIST & ALCHEMIST, INC.,

*Plaintiff,*

v.

ALURENT PRODUCTS, INC. and WILL  
CLARENT,

*Defendants.*

Civil No. 16-cv-09204-ER

**DECLARATION OF JOSHUA AAS IN  
SUPPORT OF NON-PARTY LET'S  
ENCRYPT'S MEMORANDUM OF  
LAW IN RESPONSE TO ORDER TO  
SHOW CAUSE**

Joshua Aas hereby declares as follows:

1. My name is Joshua Aas. Since 2005, I have worked in the field of Internet and Web security technology. I spent more than ten (10) years with the Mozilla Foundation and Corporation, working on Secure Sockets Layer (SSL) validation for the Firefox web browser as a senior software engineer, engineering manager, and senior technology strategist. I have also headed Mozilla's networking technology group. Prior to that, I received degrees in Computer Science and English Literature from Macalester College, where I also served as a visiting instructor in the Department of Math, Computer Science, and Statistics.

2. For the past four (4) years, I have been the Executive Director of the Internet Security Research Group, dba Let's Encrypt, a non-party to this case. In my capacity as Executive Director, I have helped to build Let's Encrypt's core technologies, administrative policies, and compliance operations from the ground up. I also helped to architect Let's Encrypt's technology stack, including technology related to receiving SSL certificate



requests, validating those requests, and issuing SSL certificates.

3. I am an expert in the area of network communications and communications security, including SSL, key-based cryptography, and related technologies. Enclosed as Exhibit A is a current copy of my *curriculum vitae*.

#### **FACTUAL BACKGROUND, LET'S ENCRYPT AND SSL CERTIFICATES**

4. Let's Encrypt is a California nonprofit corporation, with its principal place of business in San Francisco, California.

5. Let's Encrypt functions as a Certificate Authority ("CA") that, when requested, issues domain-validated SSL certificates. A CA is an entity that issues digital security certificates.

6. Transport Layer Security ("TLS") and its predecessor Secure Socket Layer (frequently referred to collectively as "TLS/SSL" or simply "SSL"), are means by which a user's communications with a website are secured from outsiders who may wish to eavesdrop on, interfere with, or alter those messages as they transit the internet. SSL operates by using a form of public-private key cryptography to securely exchange a single shared encryption key; the shared key is then used to encrypt the communications. Public Key Cryptography requires each party to have a pair of keys – one public and one private. Messages encrypted with the public key can only be decrypted with the matching private key; similarly, messages encrypted with the private key can only be decrypted with matching public key. Public keys can be shared with anyone, while private keys are kept secret. This allows for others to ensure only the desired recipient can read a message – by using the recipient's public key to encrypt the message, the sender can have confidence that only the intended recipient (who has the matching private key) can decrypt it.

7. SSL certificates are one way in which a party can share their public key (and thus



allow encrypted communications from another party). The SSL certificate contains, at a minimum, the fully qualified domain name of the website, the public key of the certificate holder, the name of the issuer of the certificate (e.g. a CA like Let's Encrypt), and the signature of the issuer.

8. Anyone can create and sign their own certificates (a “self-issued” certificate), or they can create a certificate and send it to a CA as part of a Certificate Signing Request (“CSR”) asking the CA issue a signed certificate. The issuer’s signature, contained with the SSL certificate, is not responsible for encrypting the communication channel – instead, the public-private key pair (of which the public key is contained within the certificate) and the shared secret key are responsible for encrypting the communication channel.

9. Signing an SSL certificate serves an important purpose – a certificate signed by a trusted CA can help users detect whether or not they have been tricked into communicating with a website other than the one they intended. Users can detect this by checking whether the signature on the signed certificate currently provided by the website matches the signature of a trusted CA – if the two signatures match, users can trust they are communicating with the intended website. Without a CA-signed certificate, an attacker could trick users into thinking they are visiting a particular website, while actually redirecting those users to an imposter website. Alternatively, the attacker could alter the information transmitted between the website and its users.

10. There are different types of SSL certificates, each of which carries different assurances from the CA about the certificate holder. The certificates issued by Let's Encrypt are known as “domain-validated” certificates (“DV certificates” or “DV SSL certificates”). A DV certificate is a statement by Let's Encrypt that a specified domain was under the control of the certificate’s holder at the time the holder requested the signed certificate from



Let's Encrypt. Domains provide their certificates to visitors who seek to use SSL. DV certificates do not contain any information about the identity of the holder of the certificate or make any assertions about the content available on the domain. By examining the provided certificate, its signature, and a trusted list of CAs and keys, visitors trying to connect to a domain can gain confidence that they are connecting to the domain that they intend to connect to. Unexpected changes in control of a domain, or lack of a certificate asserting domain control, could indicate a security problem, such as a compromised website, a man-in-the-middle attack, or a spoofing attack.

11. Digital security certificates are intended only to secure communications by validating the domain and encrypting the communications traffic. No CA, including Let's Encrypt, has control over how third-parties like the Defendants use a domain name, and CAs lack the ability to control content placed or maintained on any third-party website. CAs also lack the ability to render third-party websites inaccessible. DV certificates are concerned with whether a website, as viewed by a site visitor, is in fact that website (as opposed to, for example, an imposter). Their presence or absence does not affect the content of a website, and customers can continue to buy products from a site regardless of whether or not a CA revokes the certificates.

12. Let's Encrypt does not charge a fee for its security certificate services, and provides them on an equal and automated basis to all members of the public who request them. We do this because we want to create a more secure and privacy-respecting Web. Only 58% of all website traffic is protected by SSL security technology, and as security threats proliferate on the internet it is critically important that this number continue to grow.

### **SSL, WEBSITES, AND CREDIT CARD PAYMENTS**

13. A website's DV certificate (or lack thereof) is typically unrelated to that website's



ability to accept credit card transactions. Let's Encrypt certificates are not specific to payment processing, and are not specifically provided for the purpose of payment processing.

14. It is common practice for websites to use a third-party payment processor, rather than process transactions themselves, in which case it is that third party payment processor's security certificate – not the DV SSL certificate used to secure the website itself – that is used to secure the payment. For example, I understand from Plaintiff's briefing that Amazon Payments, Inc., at one point handled credit card transactions for the website at issue; in such cases, it would be common for the security certificate associated with Amazon Payments to secure any communications between the website and Amazon payments.

15. The November 10, 2016, privacy policy for herbal-chemist.com seems to confirm that credit card transactions were being handled by an outside vendor, noting that "[y]our credit card information is transmitted securely to our third part [sic] processing provider in compliance with Payment Card Industry standards." See Costa Decl., Exhibit A. Let's Encrypt does not offer payment processing services of any kind, including as described in Defendants' previous privacy policy.

16. Website owners can also facilitate credit card transactions without an SSL security certificate, or using a self-signed certificate (though some browsers may present a warning in these circumstances). Even today, many websites that accept payment by credit card do not use SSL, and many others only use SSL only for certain pages within their website.

17. SSL certificates can be revoked – but this does not remove the revoked certificate from circulation or prevent the use of the revoked certificate by the certificate holder. Instead, visitors to websites must check either a Certificate Revocation List or an Online Certificate Status Protocol server to determine if a certificate has been revoked. The



majority of web browsers do not check revocation status, in part for privacy reasons.

18. Websites are not required to enable SSL or acquire an SSL security certificate, and revocation of the SSL certificate would do nothing to affect ownership of a domain name, to change the allegedly infringing domain name visitors are presented with when arriving at a website, to alter the content and products available at a domain, or to inhibit a website's ability to accept credit card transactions.

**LET'S ENCRYPT HAS NO RELATIONSHIP TO DEFENDANTS OR NON-PARTY NAMECHEAP**

19. Let's Encrypt is not a party to this case, nor a director, principal, officer, agent, representative, servant, employee, attorney, successor, or assign of any Defendant in the case. Let's Encrypt is incapable of rendering Defendants' website inaccessible, or removing any content from their website. Other than providing automated issuance of DV SSL security certificates that recipients can use to secure and authenticate communications with their website, Let's Encrypt does not have any business relationship with the Defendants whatsoever.

20. Let's Encrypt has never advertised, promoted, hosted, or sold Defendants' allegedly infringing material on our website.

21. Let's Encrypt has not issued an SSL security certificate to Namecheap, Inc., or its namecheap.com domain, and so cannot obey the proposed order regarding withdrawing the SSL security certificate from Namecheap. Namecheap's SSL security certificate appears to have been issued by Comodo Group, Inc., a company unaffiliated with Let's Encrypt.

**CONTACTS WITH NEW YORK**

22. Let's Encrypt does not specifically target the State of New York as a place of business, nor does it have any continuous or systematic contact with the state. Let's Encrypt



does not maintain any office or office space in the State of New York and does not have any employees or agents in New York. Let's Encrypt does not own, nor has it ever owned, real or personal property located in the State of New York. Let's Encrypt maintains no telephone number or mailing address in the State of New York, and our website does not list any New York contact information.

23. Let's Encrypt currently is not, nor has it ever been, authorized or licensed to do business in the State of New York. Let's Encrypt does not have an agent for service of process in the State of New York. Let's Encrypt does not have a bank account in the State of New York. Let's Encrypt does not incur or pay, nor has it ever incurred or paid, taxes in the State of New York.


24. Let's Encrypt does not have, nor has it ever had, any member, parent, or subsidiary corporation located in the State of New York.

25. Let's Encrypt does not direct advertisement to, or solicit business specifically in, the State of New York, and does not instruct any person or entity to advertise or solicit business in the State of New York on its behalf.

26. Let's Encrypt's only contact with the State of New York is via our generally accessible website and free DV SSL security certificates services, which are available to residents in New York as they are available to residents in all other jurisdictions with access to the internet.

I swear under penalty of perjury under the laws of the United States that the foregoing is true and accurate to the best of my knowledge, information, and belief.

Date: Minneapolis, MN  
August 7, 2017

  
Joshua Aas



**CERTIFICATE OF SERVICE**

I hereby certify that this document filed through the CM/ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants. As agreed between Let's Encrypt and Plaintiff, an electronic copy of this document will also be served on counsel for Plaintiff via email.

August 7, 2017

\_\_\_\_\_  
/s/  
Warren Stramiello